



API-standaard voor logging van verwerkingen

Informatiesessie leveranciers
10 maart 2021

Huishoudelijk

- Camera en microfoon uit
- Vragen stellen via de **chat** (worden gemodereerd)
- Sheets (en vragen / antwoorden) worden na afloop gedeeld

Context

- Opdracht en scope
- Aanpak en realisatie
- AVG: de letter versus de geest

Uitwerking

- Uitgangspunten
- Begrippen
- Voorbeelden
- Maturity Levels
- Ontwerpbesluiten

Uitzoomen

- Architectuur
- Waar staan we nu



Context

Opdracht en scope





Realiseer een API-standaard die door zowel bestaande als nieuw te ontwikkelen informatiesystemen gebruikt kan worden om invulling te geven aan de AVG-verplichting verantwoording af te kunnen leggen over de verwerking van persoonsgegevens (de zogenaamde AVG Verantwoordingsplicht).



Context

Aanpak realisatie API-standaard





Overwegingen bij de aanpak

- De API-standaard is van belang voor alle informatiesystemen die persoonsgegevens verwerken, zowel huidige als nieuw te ontwikkelen. Daarmee is de standaard voor (bijna) alle leveranciers relevant. De kwaliteit van de API-standaard is dus extreem belangrijk.
- Kwaliteit begint bij een stevige fundering!
- Om een stevige fundering te kunnen maken moet bekend zijn wat de fundering moet kunnen dragen. Een gedegen analyse van (toekomstige) eisen en wensen was dus vereist.





Gevolgde aanpak

- Interviews met een aantal gemeentelijke FG/PO's ten aanzien van hun eisen en wensen op het gebied van logging van verwerkingen en het verwerkingsactiviteitenregister
- Daarna een “ouderwetse” informatieanalyse uitgevoerd
 - Analyse bronbestanden (o.a. (U)AVG, IBD handreikingen, VNG-R architectuurdocumenten)
 - Requirements gedestilleerd uit bronbestanden
 - Cases uitgeschreven, onder andere
 - Bijhouding en opvragen van logginggegevens
 - Vertrouwelijke logging en Bewaartermijnen
 - Onderscheid privaat- en publiekrechtelijke verwerkingen
 - Ketenproblematiek
 - Ontwerpbesluiten genomen en aanbevelingen gedaan
 - Gegevensmodel, gegevenswoordenboek en OAS-specificaties opgesteld
 - Architectuurdocumentatie opgesteld met beschrijving inrichtingsscenario's



Context

AVG: de letter versus de geest





AVG Verantwoordingsplicht

- De AVG legt een verwerkingsverantwoordelijke de verantwoordelijkheid op om aan te tonen dat deze bij de verwerking van persoonsgegevens aan de privacyregels voldoet;
- Een verwerkingsverantwoordelijke moet kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid;
- Volgens art. 4 lid 2 AVG is het verwerken van persoonsgegevens: *‘elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.’*





AVG Verantwoordingsplicht

- De AVG zegt niet *hoe* een verwerkingsverantwoordelijke invulling moet geven aan het voldoen aan de privacyregels;
- De AVG geeft wel in een aantal wetsartikelen aan welke informatie vastgelegd moet worden, en welke op verzoek van de burger gedeeld moet worden;





AVG: Inzage informatie door de burger

Artikel 13, 14 en 15 van de AVG geven aan welke informatie met de burger gedeeld moet worden als deze hierom verzoekt.

- de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking
- de betrokken categorieën van persoonsgegevens
- de bron waar de persoonsgegevens vandaan komen
- de bewaartermijn van de gegevens
- de ontvangers of categorieën van ontvangers van de persoonsgegevens
- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke
- de contactgegevens van de functionaris voor gegevensbescherming





AVG: de letter versus de geest

- In het kader van Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene stelt de AVG in Artikel 12:

“De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt.”

- Het is duidelijk de intentie van de wetgever dat de burger bij een inzageverzoek voorzien wordt van informatie die door de burger ook begrepen kan worden. Dit stelt eisen aan de gegevens die ten aanzien van een verwerking vastgelegd worden.



Uitwerking

Uitgangspunten opzet API-standaard





Perspectief van de burger is leidend

- De burger moet bij inzage van de verwerkingen, bijvoorbeeld via de gemeentelijke persoonlijke internet pagina, informatie zien die hij of zij kan begrijpen.
- Hoe meer duiding wordt gegeven aan een verwerking bij de vastlegging hoe beter de burger de verwerking zal begrijpen.
- Hoe duidelijker de verwerkingen aan burgers worden gepresenteerd, hoe minder vragen vanuit de burger aan de gemeente worden gesteld.





Het doel van de logging is duiden, niet reconstrueren

- Informatie die wordt gelogd is bedoeld om de actie te 'duiden' (te beschrijven);
- Het log is geen auditlog en is niet bedoeld om exact 'een beeld' te kunnen reconstrueren;
- Reconstructie vraagt o.a. om:
 - ophalen van de gegevens uit het bronsysteem op het moment dat deze bekeken zijn;
 - de software die gebruikt werd op het moment dat de informatie uit het bronsysteem werd gehaald;
 - identieke inrichting van autorisatie en infrastructuur;
 - onwijzigbare opslag, dus ook geen (structuur)wijzigingen en daarbij behorende conversies.





In de opzet van de API-standaard is vanaf het ontwerp rekening gehouden met de bescherming van de privacy.

Voorbeelden

- Geen opname van persoonsgegevens in de API behalve identificerende sleutels.
- Gebruik van aparte scopes voor loggen en opvragen van 'gewone' en vertrouwelijke acties.
- Aanbevelingen ten aanzien van encryptie van het BSN bij opslag in het logregister.
- Bescherming van de identiteit van de gemeentelijk medewerker.
- Mogelijkheid tot alternatieve identificatie voor verwerking waarvoor het BSN niet mag worden gebruikt (bijvoorbeeld privaatrechtelijke verwerkingen).





Faciliteren laagdrempelige inbouw

- De API-standaard moet dusdanig zijn opgezet dat iedere leverancier de API-standaard op een eenvoudige manier kan implementeren.
- Zo min mogelijk verplichte velden zodat verwerkingen altijd vastgelegd kunnen worden. Het is beter om een verwerking met een minimale set gegevens vast te leggen dan een verwerking niet vast te leggen;
- Geen impact op bestaande diensten die gegevens verwerken
 - Geen specifieke payload attributen voor logging;
 - Specifieke attributen voor logging worden via de http-header doorgeven;





Implementatie laten we over aan de markt

- De API-standaard schrijft geen verplichtingen voor ten aanzien van de wijze van implementatie van de API-standaard;
- Geen beschrijving van de functionaliteit van een verwerkingenlog buiten de in de API-standaard gespecificeerde functies;
- Wel beschrijving van scenario's voor binnengemeentelijke implementatie en best-practices en aanbevelingen op bijvoorbeeld het gebied van privacy by design;






Uitwerking

Begrippen



- **Verwerkingsactiviteit** = Een soort verwerking 
 - Het gemeentelijk register van verwerkingsactiviteiten bevat een opsomming van alle soorten verwerkingen die een gemeente uitvoert.
- **Verwerking** = Een concrete verwerking 
 - Een concreet verzoek, zaak, onderzoek, proces...
 - Het verwerkingenlog bevat metagegevens over verwerkingen
- **Actie** = Een concrete operatie op een systeem
 - Registreren, opvragen, aanpassen, corrigeren van gegevens
 - Onderdeel van een verwerking



Register van verwerkingsactiviteiten

	A	B	H	L	M	N	O	R	S
	ID	Hoofdproces	Naam verwerking	Doeleinde	Grondslag	Uitleg	Categorieën Betrokkenen	Categorieën persoonsgegevens	Categorieën Ontvangers
1									
83	80	Burgerzaken	Register burgerlijke stand + huwelijksdossiers	Opmaken aktes van de burgerlijke stand	Wettelijke verplichting	BW, Besluit Burgerlijke Stand (BBS)	Burgers	Alle categorieën	Ministerie van justitie Buitengewone ambtenaren burgerlijke stand
85	82	Burgerzaken	Naamkeuze kind	Verklaren van de keuze voor de naam van een pasgeboren baby	Publieke taak	Art. 1:4 BW	Aanvragers Kinderen	Persoonlijke gegevens	
86	83	Burgerzaken	Geslachtsnaamwijziging	Wijzigen van geslachtsnaam	Wettelijke verplichting	Art. 1:5, 1:7, 1:20 lid 1 sub a en 1:20a lid 1 BW	Aanvragers Kinderen	Persoonlijke gegevens	Andere gemeenten, rechtbank
87	84	Burgerzaken	Geslachtswijziging	Wijziging van het geslacht	Wettelijke verplichting	Art. 1:28b BW	Aanvrager	Persoonlijke gegevens	Andere gemeenten, rechtbank
94	91	Burgerzaken	BRP registratie	Bijhouding van persoonslijsten van ingezetenen	Wettelijke verplichting	Wet basisregistratie personen	Burgers		

Granulariteit in register van verwerkingsactiviteiten zal vaak niet uniform zijn.

- Verwerkingsactiviteit = Een soort verwerking (Type)
- Verwerking = Een concrete verwerking (Instantie)
- + Handeling = Een stap binnen het verwerkingsproces
- Actie = Een concrete operatie op een systeem

Extra niveau (optioneel) om
verschillen in granulariteit
op te vangen



Voorbeelden begrippen

	Case 1	Case 2	Case 3	Case 4	Case 5
Verwerkings-Activiteit	Register burgerlijke stand + huwelijksdossiers	Geslachtswijziging	Registratie verhuizingen	Fraudeonderzoek sociale zekerheid	Verstrekken van informatie aan derden
Verwerking	Huwelijk	Geslachtswijziging	Registratie verhuizing	Onderzoek	Bevraging door derde
Handeling	<ul style="list-style-type: none"> - Intake - Ondertrouw - Opmaken akten - Voorbereiding ceremonie - Registratie huwelijk 	<ul style="list-style-type: none"> - Wijziging geslacht - Wijziging voornaam - Aanpassen historie 	(Registratie verhuizing)	<ul style="list-style-type: none"> - Verzamelen gegevens - Verificatie ... 	(Bevraging door derde)
Actie	<ul style="list-style-type: none"> - Zoeken personen - Ophalen pers. gegevens - Opslaan pers. gegevens 	<ul style="list-style-type: none"> - Ophalen pers. gegevens - Opslaan pers. gegevens 	<ul style="list-style-type: none"> - Ophalen pers. gegevens - Opslaan pers. gegevens 	...	Ophalen pers.gegevens





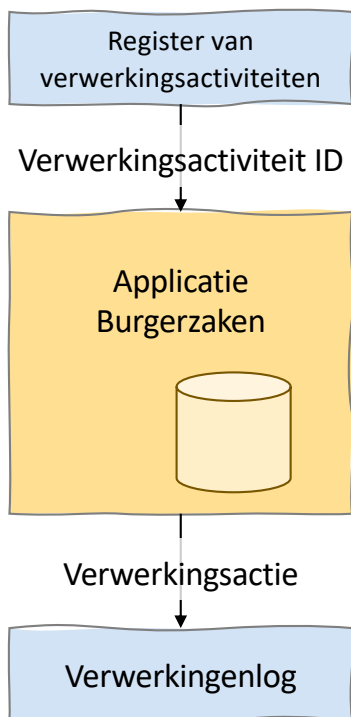
Uitwerking

Voorbeelden





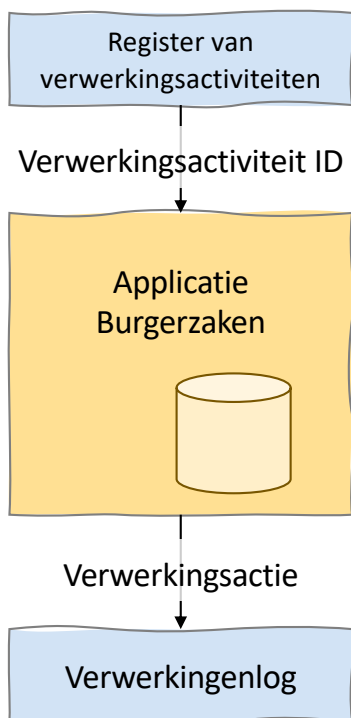
Logging van verwerkingen



Het gaat in de voorbeelden die volgen om de functionaliteit en de gegevens, niet om de architectuur van de voorzieningen en registers.



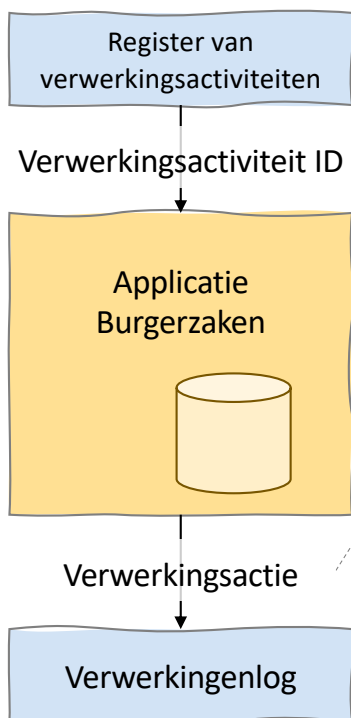
Register van verwerkingsactiviteiten



Verwerkingsactiviteit	
ID	{VA-1}
Naam	Register burgerlijke stand + huwelijksdossiers
Verantw. organisatie	Gemeente X
Verantw. bestuursorgaan	College van B&W
Doel	Opmaken aktes van de burgerlijke stand
Grondslag	Wettelijke verplichting
Toelichting grondslag	BW, Besluit Burgerlijke Stand
Bewaartermijn	75 jaar
Herkomst gegevens	Betrokkene, BRP
Cat. persoonsgegevens	Alle categorieën
Cat. ontvangers	Ministerie van justitie, Buitengewone ambtenaren burgerlijke stand
...	



Verwerkingenlog – Verwerkingsactie Minimaal



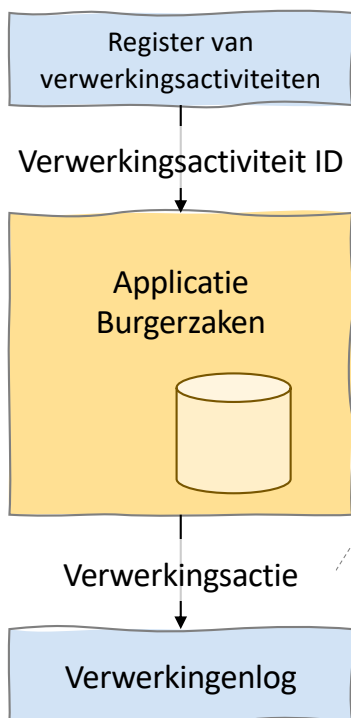
Verwerkingsactie	
Actie Naam	
Handeling Naam	
Verwerking Naam	
Verwerking ID	
Verwerkingsactiviteit ID	{VA-1}
Verwerkingsactiviteit URL	https://...
Vertrouwelijkheid	Normaal
Bewaartermijn	
Uitvoerder	{OIN Uitvoerder}
Systeem	Burgerzakenapplicatie v2.1
Gebruiker	{UUID gebruiker}
Gegevensbron	Burgerzaken DB
Tijdstip	2024-04-05T14:35:42+01:00
Verwerkt object	Persoon, BSN, 5872525
Verwerkt object	Persoon, BSN, 6235489

Register burgerlijke stand
+ huwelijksdossiers





Verwerkingenlog – Verwerkingsactie Uitgebreider

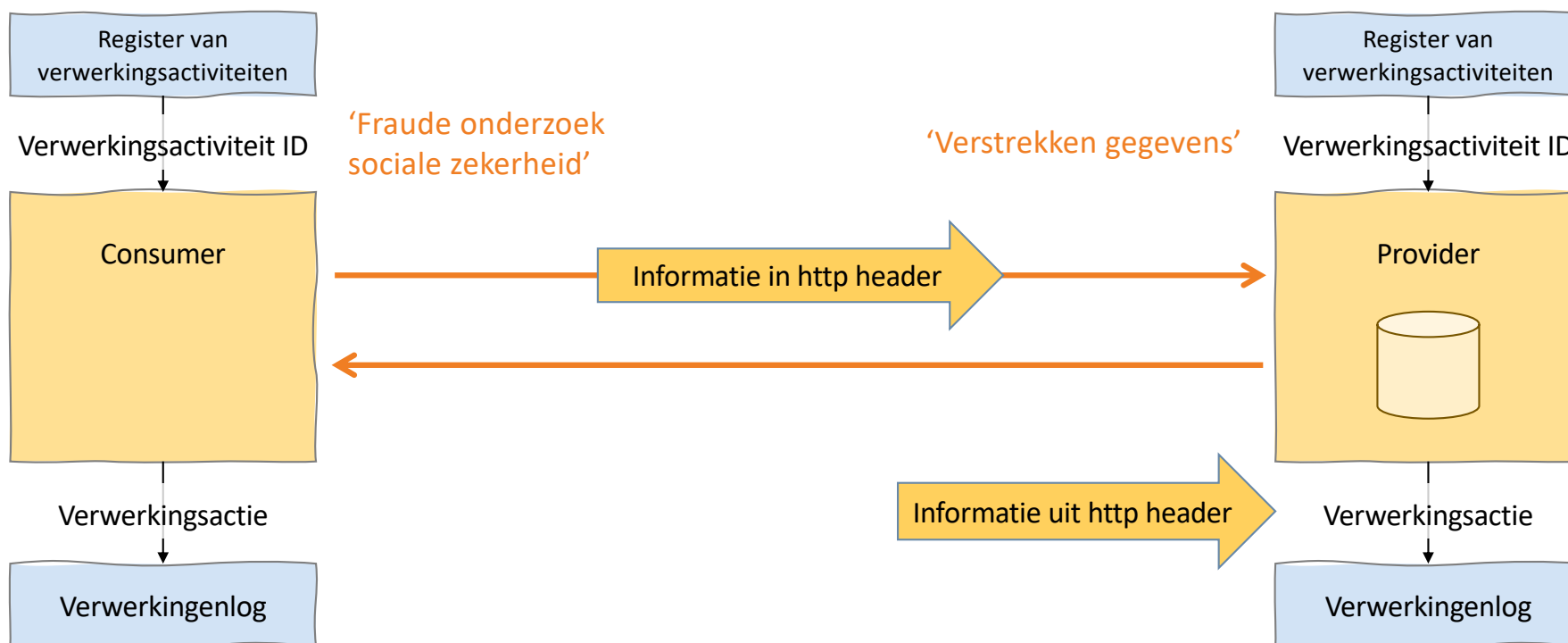


Verwerkingsactie	
Actie Naam	Opvragen persoonsgegevens
Handeling Naam	Vorbereiding huwelijksakte
Verwerking Naam	Huwelijk
Verwerking ID	
Verwerkingsactiviteit ID	{VA-1}
Verwerkingsactiviteit URL	https://...
Vertrouwelijkheid	Normaal
Bewaartermijn	...
Uitvoerder	{OIN Uitvoerder}
Systeem	Burgerzakenapplicatie v2.1
Gebruiker	{UUID gebruiker}
Gegevensbron	Burgerzaken DB
Tijdstip	2024-04-05T14:35:42+01:00
Verwerkt object	Persoon, BSN, 5872525, Getuige
Verwerkt object	Persoon, BSN, 6235489, Getuige

Register burgerlijke stand
+ huwelijksdossiers

AVG Artikel 12: “De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een **beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt.**”

Consumer / Provider – Verschillende organisaties





Informatie in http header



Http Header	
OIN	{OIN Gemeente X}
Verwerkingsactiviteit ID	{VA-C} <div>Fraude onderzoek sociale zekerheid</div>
Verwerkingsactiviteit URL	https://...
Verwerking ID	{UUID van zaak/dossier/...}
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar

Verwerkingsactie	
Actie Naam	Ophalen persoonsgegevens
Handeling Naam	-
Verwerking Naam	Bevraging door derden
Verwerking ID	-
Verwerkingsactiviteit ID	{VA-P} <div>Verstrekken gegevens</div>
Verwerkingsactiviteit URL	https://...
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar
Uitvoerder	{OIN Uitvoerder}
Systeem	Bronregistratie Provider v3.2
Gebruiker	-
Gegevensbron	Bronregistratie DB
Tijdstip	2024-04-05T14:35:42+01:00
Verwerkt object	Persoon, BSN, 5872525
Verwerkt object	Persoon, BSN, 6235489



Informatie in http header

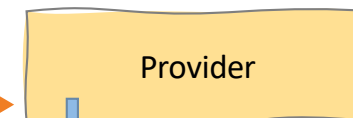
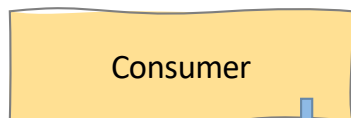


Http Header	
OIN	{OIN Gemeente X}
Verwerkingsactiviteit ID	{VA-C} <div>Fraude onderzoek sociale zekerheid</div>
Verwerkingsactiviteit URL	https://...
Verwerking ID	{UUID van zaak/dossier/...}
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar

Verwerkingsactie	
Actie Naam	Ophalen persoonsgegevens
Handeling Naam	-
Verwerking Naam	Bevraging door derden
Verwerking ID	-
Verwerkingsactiviteit ID	{VA-P} <div>Verstrekken gegevens</div>
Verwerkingsactiviteit URL	https://...
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar
...	
Soort afnemer ID	OIN
Afnemer ID	{OIN Gemeente X}
Verwerkingsactiviteit ID afnemer	{VA-C}
Verwerkingsactiviteit URL afnemer	https://...
Verwerking ID afnemer	{UUID van zaak/dossier/...}



Http Header	
OIN	{OIN Gemeente X}
Verwerkingsactiviteit ID	{VA-C}
Verwerkingsactiviteit URL	https://...
Verwerking ID	{UUID van zaak/dossier/...} ←
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar



Informatie in http header

Verwerkingsactie	
Actie Naam	Opvragen persoonsgegevens
Handeling Naam	Initiatie onderzoek
Verwerking Naam	Onderzoek uitkeringsfraude
Verwerking ID	{UUID van zaak/dossier/...} ←
Verwerkingsactiviteit ID	{VA-C} - Fraude onderzoek
Verwerkingsactiviteit URL	https://... sociale zekerheid
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar
Uitvoerder	-
Systeem	AppSociaal v9.5
Gebruiker	{UUID gebruiker}
Gegevensbron	AppSociaal DB
Tijdstip	2024-04-05T14:35:42+01:00
Verwerkt object	Persoon, BSN, 5872525
Verwerkt object	Persoon, BSN, 6235489

Verwerkingsactie	
Actie Naam	Ophalen persoonsgegevens
Handeling Naam	-
Verwerking Naam	Bevraging door derden
Verwerking ID	-
Verwerkingsactiviteit ID	{VA-P} - Verstrekken gegevens
Verwerkingsactiviteit URL	https://...
Vertrouwelijkheid	Vertrouwelijk
Bewaartermijn	20 jaar
...	
Soort afnemer ID	OIN
Afnemer ID	{OIN Gemeente X}
Verwerkingsactiviteit ID afnemer	{VA-C}
Verwerkingsactiviteit URL afnemer	https://...
Verwerking ID afnemer	{UUID van zaak/dossier/...} ←

Het doorgeven en opslaan van het Verwerking ID is noodzakelijk om op een later moment de vertrouwelijkheid te kunnen laten vervallen en/of de bewaartermijn op te geven of aan te passen.

Uitwerking

Maturity Levels



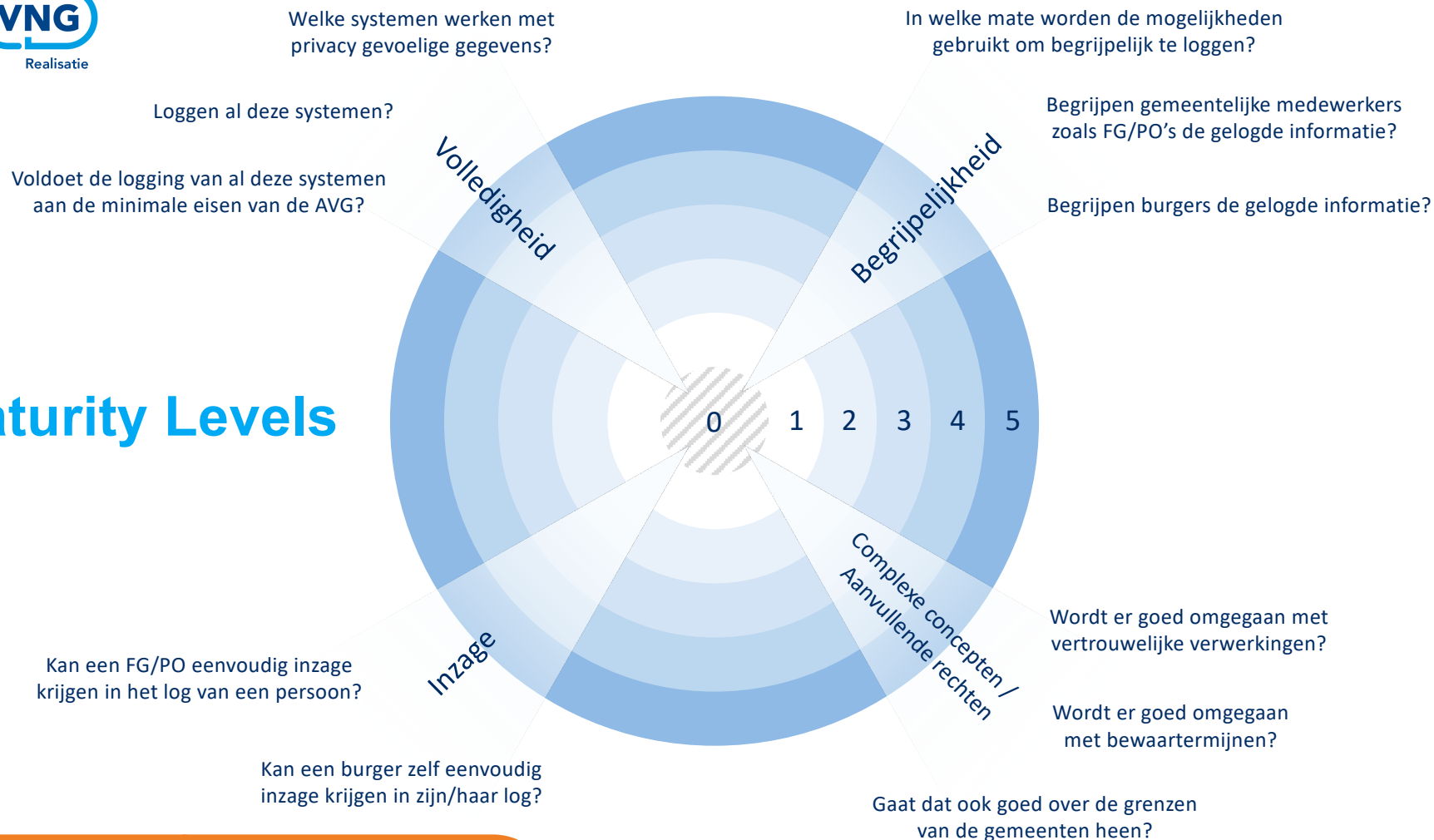


Waarom Maturity Levels?

- Niet realistisch om direct de maximale mogelijkheden van de standaard verplicht te stellen.
- Om gefaseerde invoering mogelijk te maken is daarom veel optioneel.
- Met behulp van concreet gedefinieerde maturity levels wildgroei bij gebruik voorkomen.



Maturity Levels





Uitwerking

Ontwerpbesluiten





Van begrippen naar conceptueel model

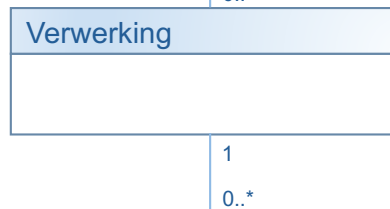
Verwerkingsactiviteit



Type

Soort verwerking

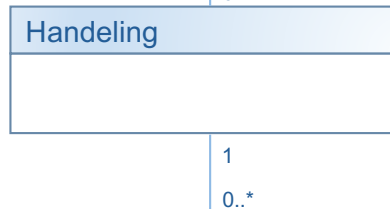
Verwerking



Instantie

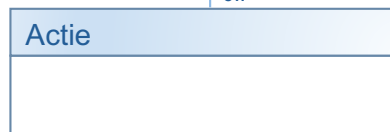
Concrete verwerking

Handeling



Stap in verwerkingsproces

Actie



Operatie op systeem



Van conceptueel naar uitwisselingsmodel

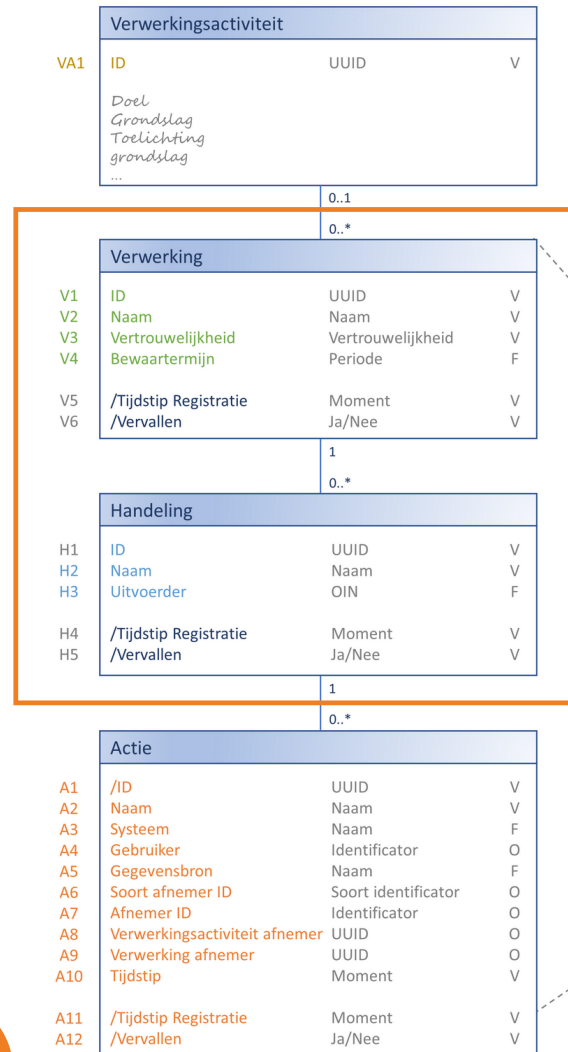
Denormalisatie:

Verwerking, Handeling en Actie zijn samengevoegd tot Verwerkingsactie.

Belangrijkste overweging:

De objecten Verwerking en Handeling zijn lang niet altijd aanwezig en dus optioneel.

Conceptueel model



Uitwisselingsmodel

Verwerkingsactie			
A1	/Actie ID	UUID	V
A2	Actie Naam	Naam	F
H2	Handeling Naam	Naam	F
V2	Verwerking Naam	Naam	F
V1	Verwerking ID	UUID	F
VA1	Verwerkingsactiviteit ID	UUID	F
	Verwerkingsactiviteit URL	URL	F
V3	Vertrouwelijkheid	Vertrouwelijkheid	V
V4	Bewaartermijn	Periode	F
H3	Uitvoerder	OIN	F
A3	Systeem	Naam	F
A4	Gebruiker	Identificator	O
A5	Gegevensbron	Naam	F
A6	Soort afnemer ID	Soort identificator	O
A7	Afnemer ID	Identificator	O
A8	Verwerkingsactiviteit ID afnemer	UUID	O
	Verwerkingsactiviteit URL afnemer	URL	O
A9	Verwerking ID afnemer	UUID	O
A10	Tijdstip	Moment	V
A11	/Tijdstip Registratie	Moment	V
A12	/Vervallen	Ja/Nee	V

In implementatie nog verder normaliseren?

N.B. De implementatie wordt niet voorgeschreven vanuit de standaard!

Verwerkt object (Persoon)

- Optie 1: Records maken met daarin telkens één Verwerkt object en de bijbehorende Verwerkingsactie.

Punt van aandacht: Stel er wordt als actie gelogd dat een zoekoperatie drie personen heeft teruggegeven en dit wordt opgeslagen in drie aparte logrecords. Deze drie records moeten dan wel dezelfde Actie ID hebben!

- Optie 2: Binnen Verwerkingsactie een herhalende groep van Verwerkte objecten: Niet handig omdat Verwerkte objecten (personen) een primaire zoekingang zijn!

Verwerkt soort gegeven

- Binnen een logrecord een herhalende groep met Verwerkte soorten gegevens lijkt geen probleem. Verwerkt soort gegeven is geen zoekingang en het lijkt onwaarschijnlijk dat dit ooit een zoekingang gaat worden.

Verwerkingsactie		
/Actie ID	UUID	V
Actie Naam	Naam	F
Handeling Naam	Naam	F
Verwerking Naam	Naam	F
Verwerking ID	UUID	F
Verwerkingsactiviteit ID	UUID	F
Verwerkingsactiviteit URL	URL	F
Vertrouwelijkheid	Vertrouwelijkheid	V
Bewaartermijn	Periode	F
Uitvoerder	OIN	F
Systeem	Naam	F
Gebruiker	Identificator	O
Gegevensbron	Naam	F
Soort afnemer ID	Soort identificator	O
Afnemer ID	Identificator	O
Verwerkingsactiviteit ID afnemer	UUID	O
Verwerkingsactiviteit URL afnemer	URL	O
Verwerking ID afnemer	UUID	O
Tijdstip	Moment	V
/Tijdstip Registratie	Moment	V
/Vervallen	Ja/Nee	V

0..1

0..*

Verwerkt object		
Objecttype	Objecttype	V
Soort object ID	Soort identificator	V
Object ID	Identificator	V
Betrokkenheid	Naam	F

0..1

0..*

Verwerkt soort gegeven		
Soort gegeven	Naam	V

Mapping naar REST API resources

Type	API-call
REST	POST /verwerkingsacties
REST	GET /verwerkingsacties
REST	PUT /verwerkingsacties/{actield}
REST	DELETE /verwerkingsacties/{actield}
REST	PATCH /verwerkingsacties

Verwerkingsactie		
/Actie ID	UUID	V
Actie Naam	Naam	F
Handeling Naam	Naam	F
Verwerking Naam	Naam	F
Verwerking ID	UUID	F
Verwerkingsactiviteit ID	UUID	F
Verwerkingsactiviteit URL	URL	F
Vertrouwelijkheid	Vertrouwelijkheid	V
Bewaartermijn	Periode	F
Uitvoerder	OIN	F
Systeem	Naam	F
Gebruiker	Identificator	O
Gegevensbron	Naam	F
Soort afnemer ID	Soort identificator	O
Afnemer ID	Identificator	O
Verwerkingsactiviteit ID afnemer	UUID	O
Verwerkingsactiviteit URL afnemer	URL	O
Verwerking ID afnemer	UUID	O
Tijdstip	Moment	V
/Tijdstip Registratie	Moment	V
/Vervallen	Ja/Nee	V

0..1

0..*

Verwerkt object		
Objecttype	Objecttype	V
Soort object ID	Soort identificator	V
Object ID	Identificator	V
Betrokkenheid	Naam	F

0..1

0..*

Verwerkt soort gegeven		
Soort gegeven	Naam	V

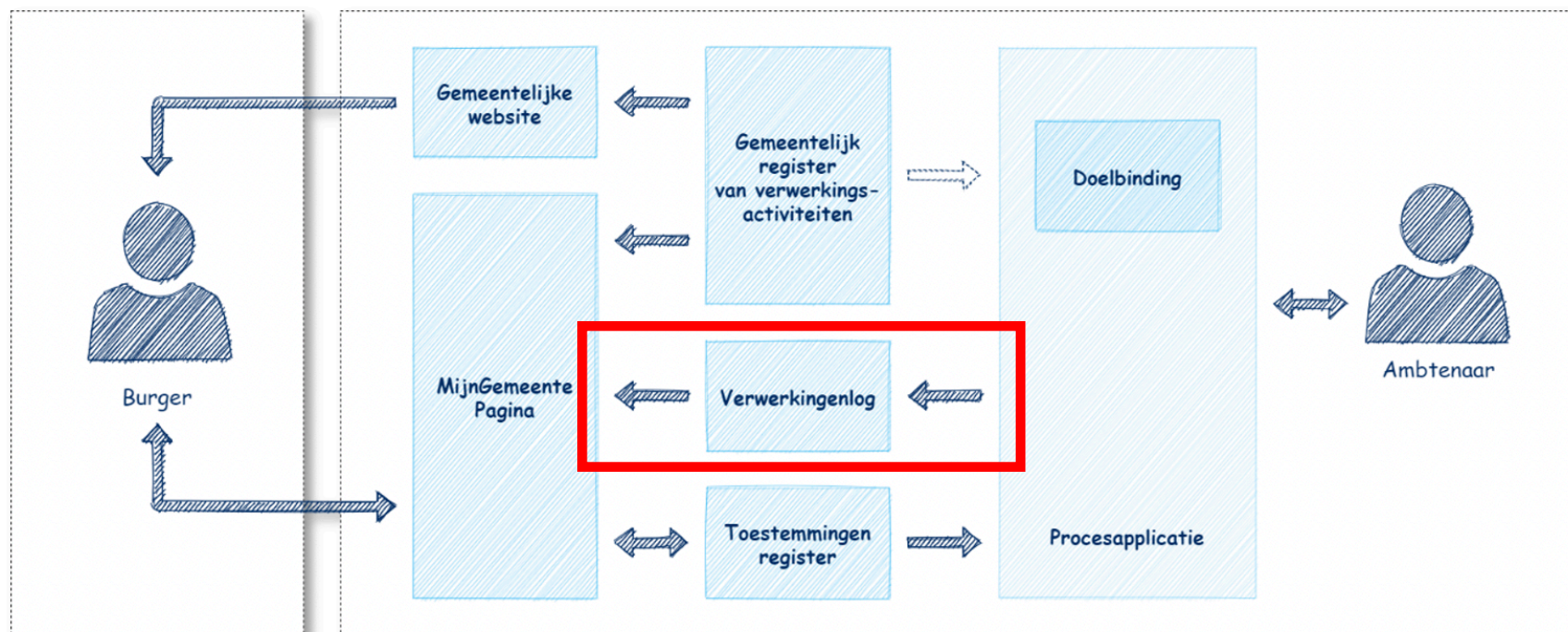


Uitzoomen

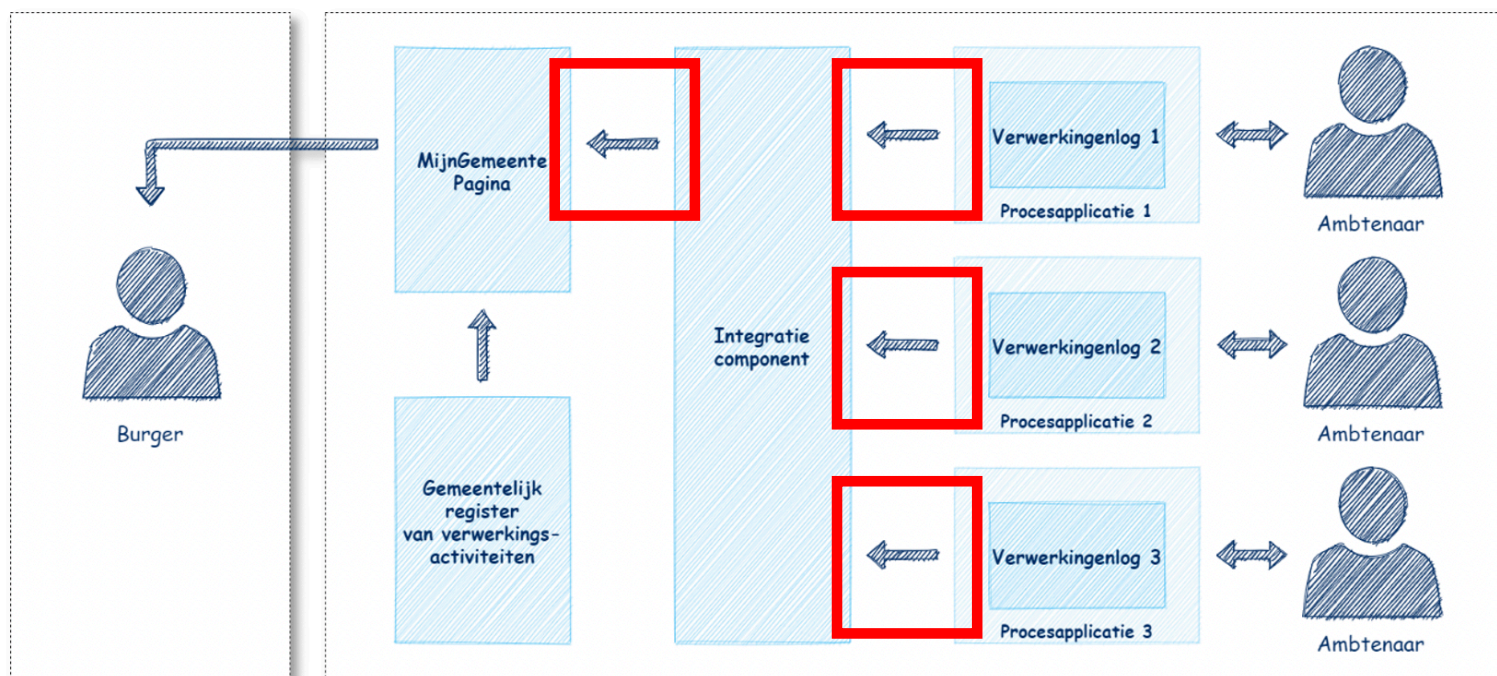
Architectuur



API-standaard in de informatievoorziening



API-standaard in de informatievoorziening (Federatieve inrichting)



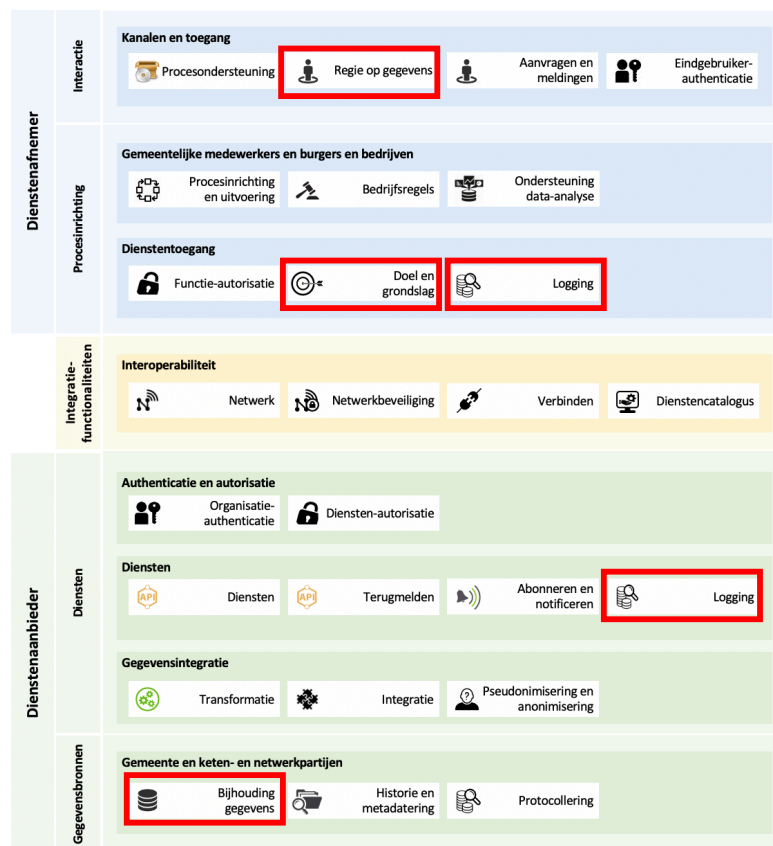


Werkingsgebied van de API-standaard

- De standaard is ontwikkeld voor het gemeentelijk domein;
 - Primair voor systemen die gegevens van personen verwerken;
 - Secundair voor systemen die gegevens van andere objecten verwerken;
- De API-standaard bevat geen gemeente-specifieke elementen en is daardoor breder toepasbaar. Zowel in het publieke- als in het private domein.



Positionering in het GEMMA Gegevenslandschap



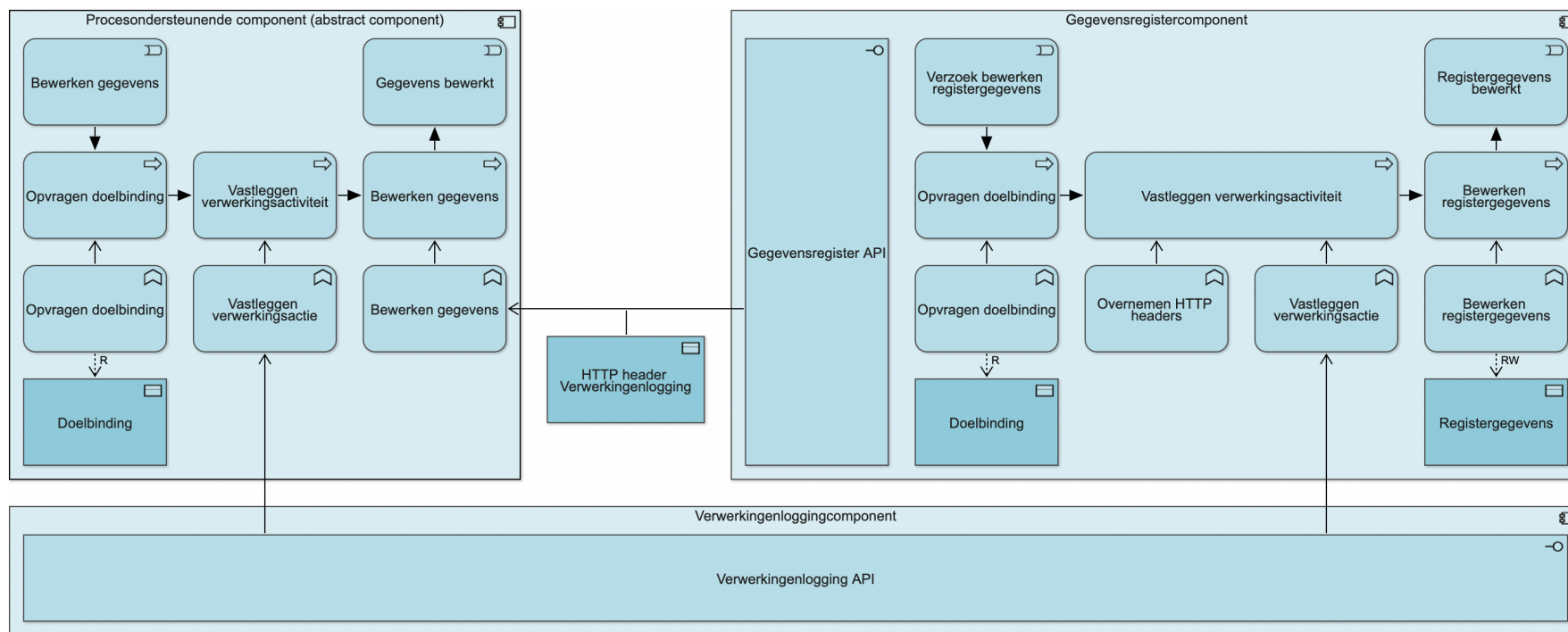


Waar worden verwerkingen vastgelegd?

- Om recht te doen aan de geest van de AVG is bij de vastlegging van een verwerking de context van de verwerking van belang. Hoe meer context hoe meer meta informatie bekend is;
- Een procesapplicatie die een verwerking uitvoert (bv het Burgerzakensysteem) kent de context van die verwerking. Bij logging vanuit dat informatiesysteem is dus het hoogst haalbare Maturity Level mogelijk;
- Logging vanuit een procesapplicatie vraagt om aanpassing van die applicatie.

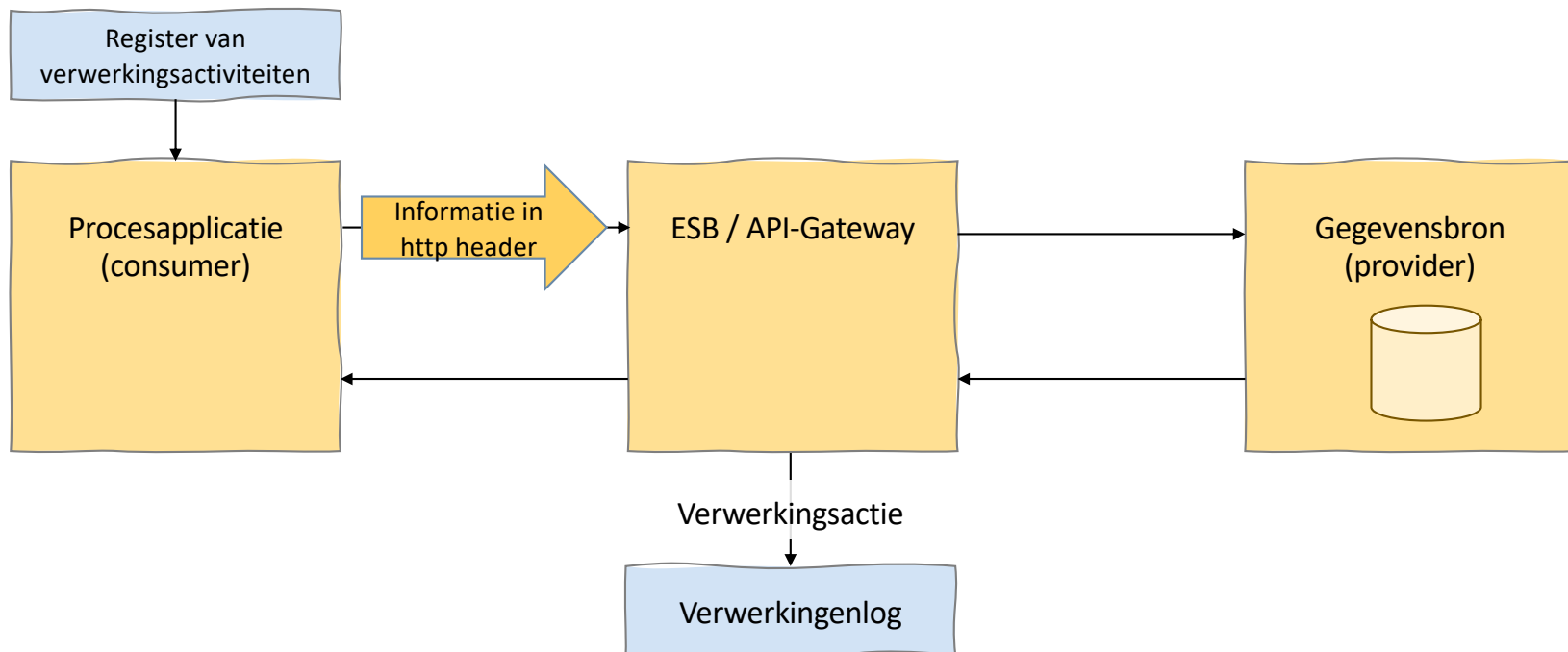


Vastlegging via procescomponent



Vastlegging via een ESB of API-Gateway

- Indien **alle** gegevensstromen van een procesapplicatie via een centraal punt lopen, bijvoorbeeld een ESB of API-gateway is het verleidelijk om de logging daar te positioneren.





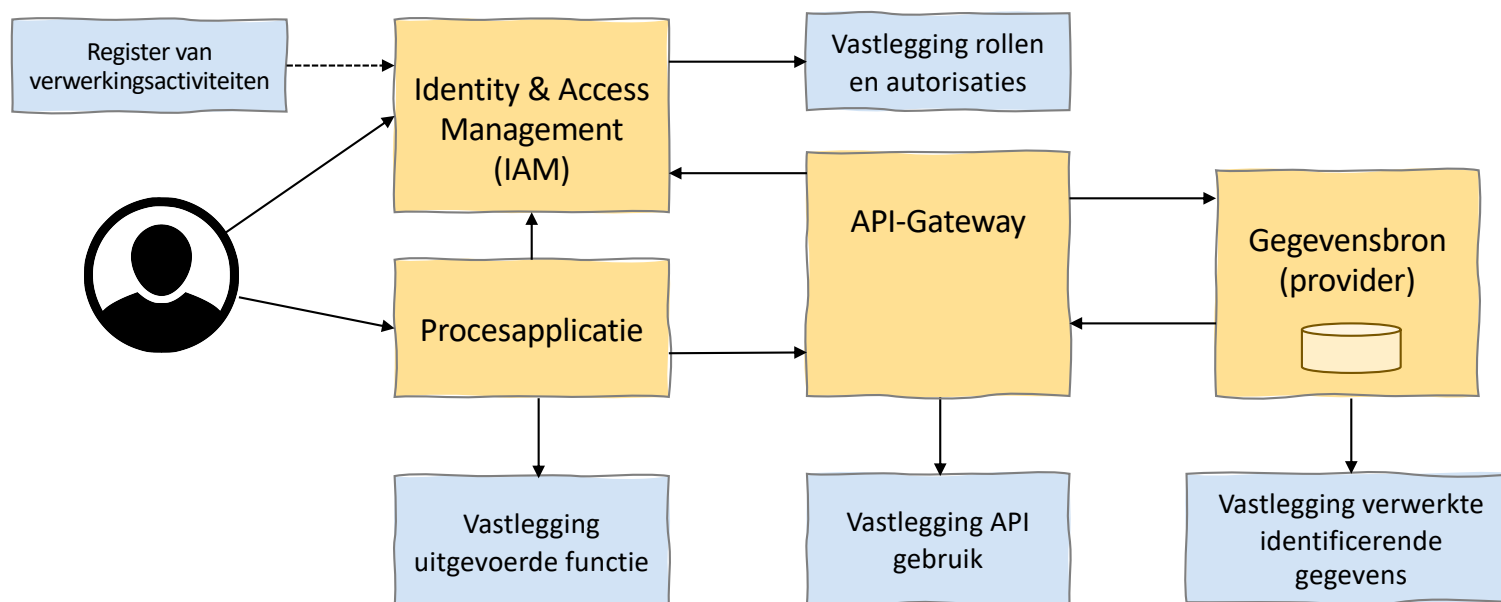
Vastlegging via een ESB of API-Gateway

- Een ESB of API-Gateway kent de context van een verwerking niet. Deze context moet dus door de procescomponent aan de ESB of API-Gateway worden meegegeven.
- Een ESB of API-Gateway heeft geen toegang tot de payload van berichten. Deze component kan dus niet bepalen welke persoonsgegevens verwerkt worden en wat de identificerende sleutel (bv BSN) van de verwerkte personen is;
- Procescomponenten moeten dus hoe dan ook vastleggen welke personen verwerkt zijn.



Vastlegging via combinatie van systemen

- In een landschap met procesapplicaties die geheel werken op basis van APIs is een alternatieve manier van vastlegging van verwerkingen denkbaar via een combinatie van vastlegging in IAM, API-Gateway, gegevensbron en procesapplicatie.





Vastlegging via combinatie van systemen

- Vastlegging van verwerkingen in een landschap waarbij informatiesystemen volledig op basis van APIs werken wordt nader onderzocht.
- Vragen die beantwoord moeten worden
 - Aan welke componenten moet een gemeente in een API-landschap invulling geven in de informatiehuishouding?
 - Wat zijn de eisen die ten aanzien van vastlegging aan deze componenten worden gesteld?
 - Wat is de samenhang van de componenten en welke koppelvlakken spelen een rol?
 - Wat is vanuit de AVG de vereiste granulariteit van rollen en autorisaties?
 - Hoe wordt de verbinding met een verwerkingsactiviteitenregister gelegd?
 - Kan via deze inrichting de verwerking van persoonsgegevens op een manier worden verantwoord die voldoet aan niet alleen de letter, maar ook de geest van de AVG?



Huidige status





Waar staan we nu?

Github

- Product visie
- Uitgewerkte informatieanalyse
- Gegevenscatalogus en gegevensmodel
- OAS-specificaties
- Quick start gids voor gemeenten
- github.com/VNG-Realisatie/gemma-verwerkingenlogging

GEMMAonline

- Inrichtingsscenario's
- Architectuurdokumentatie
- [www.gemmaonline.nl/index.php/Thema Logging en verwerkingsactiviteiten](http://www.gemmaonline.nl/index.php/Thema_Logging_en_verwerkingsactiviteiten)





Wat zijn de volgende stappen?

- Opleveren van een release kandidaat van de standaard.
- Ontwikkelen van referentieimplementatie.
- Maturity Levels uitwerken samen met gemeenten en leveranciers.
- Verwerkingenlogging API-standaard ter standaardisatie voorleggen aan het College van Dienstverleningszaken van de VNG.
- Onder de aandacht brengen van de Verwerkingenlogging API-standaard bij het Kennisplatform APIs en het Forum Standaardisatie.





Hoe kunt u bijdragen?

Github

<https://github.com/VNG-Realisatie/gemma-verwerkingenlogging>

E-mail

arnoud.quanjer@vng.nl of
standaarden.ondersteuning@vng.nl





Dank u voor uw aandacht!

